PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 — A1

(11) International Publication Number: WO 99/35582

(43) International Publication Date: 15 July 1999 (15.07.99)

(21) International Application Number: PCT/SG98/00047

(22) International Filing Date: 19 June 1998 (19.06.98)

(30) Priority Data:
9800028–4 5 January 1998 (05.01.98) SG

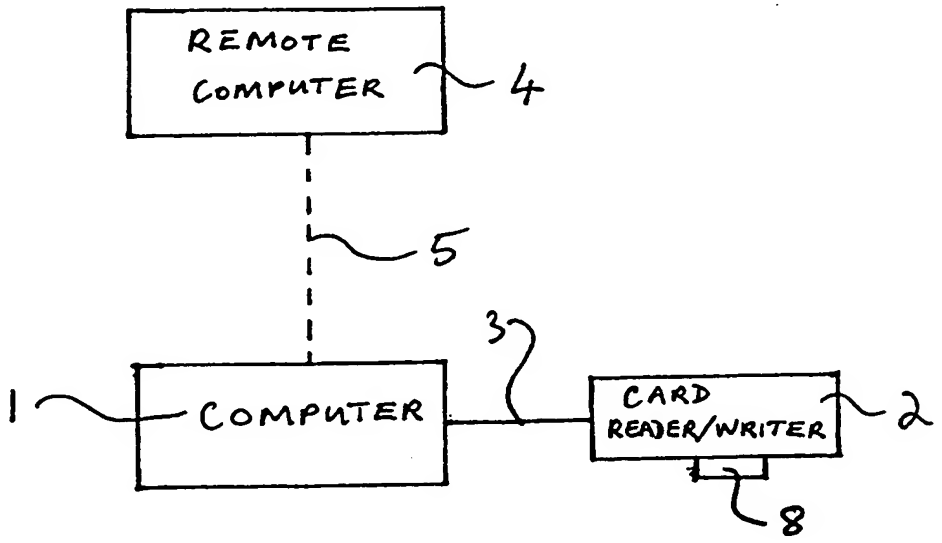
(71)(72) Applicant and Inventor: LUI, Chew, Wah [SG/SG]; 11 Yarrow Gardens, Singapore 455016 (SG).

(74) Agent: MCCALLUM, Graeme, David; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A COMPUTER SOFTWARE ACTIVATION SYSTEM AND A METHOD OF AUTHENTICATING COMPUTER SOFTWARE



(57) Abstract

A computer software activation system includes an authentication device (8), a writing device (2) for writing to the authentication device and the first computer (1) to which the writing device (2) is coupled. The first computer (1) controls the writing device (2) to write the authentication information to the authentication device (8). The authentication information written to the authentication device (8) permits corresponding software to be activated on a second computer (10).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A COMPUTER SOFTWARE ACTIVATION SYSTEM AND A METHOD OF AUTHENTICATING COMPUTER SOFTWARE

The invention relates to a computer software activation system and a method of authenticating computer software and in particular, to minimise the risk of software being illegally copied.

Software piracy is becoming a serious problem, especially in certain countries where intellectual property rights do not provide adequate protection. Even in countries where there is adequate intellectual property protection, if software piracy is endemic within the country it is extremely difficult for the true owners of the software to enforce their rights effectively. For example, in Singapore, a recent survey estimated that the rate of software piracy is approximately 50%. This means that for every genuine copy of software in Singapore there is also an illegal version. It is worth noting that Singapore is ranked as a country with a low incident of software piracy. Therefore, it can be assumed that in a number of other countries there are more illegal versions of software than legal versions.

Accordingly, the loss in revenue due to software piracy can run into millions or billions of dollars each year.

One device that is being used to try to control the problem of unauthorised copying of software is known as a "dongle".

A dongle is supplied with a software program and the software will only operate on a given computer if the corresponding dongle is simultaneously coupled to the computer while the software is running. If the correct dongle is not coupled to the computer, the software will not run on the computer. The dongle operates by storing a unique password and a routine in the software is initiated randomly to access the dongle for the password. If the dongle is not attached to the computer, the routine in the software will fail to retrieve the password and the software will shut down by itself.

However, the use of dongles has a number of problems. For example, there is a trend for users to use more and more software simultaneously on a computer and if one dongle is required for each piece of software, there may not be sufficient ports on the computer or sufficient space to have all the dongles installed simultaneously.

An alternative solution to dongles has been proposed by Microsoft (trade mark) which has attempted to reduce software piracy by creating a "registry" in its Windows 95 (trade mark) operating system. The "registry" governs where each program is installed and in what sequence these programs have to be run. The programs may be copied but the "registry" may not be copied. As the programs will not run without the registry, it is difficult to pirate software by copying the software from the hard disk on a computer. However, currently, almost all piracy is performed by duplicating the

CD-ROM which stores all the initial setup information and has copies of both the programs and the "registry".

Hence, this solution does not overcome the problem of software piracy by copying of CD-ROMs containing the software.

In accordance with a first aspect of the present invention, a computer software activation system comprises an authentication device, a writing device for writing to the authentication device, the writing device being coupled to a first computer, the first computer controlling the writing device to write authentication information to the authentication device, the authentication information written to the authentication device permitting corresponding software to be activated on a second computer.

An advantage of this aspect of the invention is that by providing an authentication device for the software the right of a user to run the software can be authenticated before or during activation of the software.

In accordance with a second aspect of the present invention, a method of authenticating computer software comprises inserting an authentication device into an authentication device reader coupled to a computer on which the software is installed, the computer obtaining, in response to a request from the software for authentication information, from the

authentication device reader, the authentication information from the authentication device prior to or during initialisation of the software, the computer supplying the authentication information to the software and the software confirming to the computer that the authentication information from the authentication device permits the software to be run on the computer.

Typically, the computer in the second aspect of the invention is the second computer in the first aspect of the invention.

Preferably, the first computer may access a remote computer to obtain authentication information from the remote computer, which the first computer then writes to the authentication device via the writing device.

Preferably, the connection between the first computer and the remote computer is a secure connection and information passed between the remote computer and the first computer may be encrypted.

Typically, the authentication device may store authentication information relating to a number of different computer software programs.

Preferably, the authentication device contains a processor, and may be, for example, a device known as a "smart card" or a "Java card".

Preferably, the authentication information comprises a password.

Typically, the software is encrypted and the authentication information may further comprise a decryption key to permit decryption of the software.

In addition, or as an alternative, the authentication information may comprise a portion of the software without which the software will not run.

The software for use with the authentication device may be installed in the computer using any conventional memory device, such as a magnetic disk or CD-ROM. Alternatively, the software may be down loaded from a remote location, for example, via the Internet.

In a further alternative, the software may be located on a network server which is accessed by a user.

An example of a system for activation of software and a method of software authentication will now be described with reference to the accompanying drawings, in which:

Figure 1 is a schematic block diagram illustrating a system for initialising an authentication device; and

Figure 2 is a schematic block diagram showing a system for using software in combination with the

authentication device.

Figure 1 shows a computer 1 which is connected to a smart card reader/writer 2 via a connection 3. The computer 1 is also capable of accessing a remote computer 4 via a telecommunication link 5. Telecommunication link 5 may be a dedicated ISDN line or may include modems and a conventional telephone line. Alternatively, the telecommunication link 5 may be via the Internet.

In use, a software manufacturer would use the system by providing software on for example, on a CD-ROM. The software on the CD-ROM would be encrypted. The software is encrypted such that each CD-ROM requires a separate decryption key to decrypt the software on it. In addition, each CD-ROM produced by the software manufacturer is assigned a unique identification code.

When a purchaser buys software on a CD-ROM from a retailer, the retailer must be licensed and registered with the software manufacturer. If the retailer is registered he will have been assigned a user-id and a secure password to access the remote computer 4 of the manufacturer where there is a registry. The purchaser must have in his possession an authentication device 8 such as a smart card or a Java card 8 (see Fig. 1) that has an indelible record of his identity (for example, similar to the Netrust card in Singapore). If he does not have one, the retailer may issue one to him.

An advantage of using a smart card or Java card 8 is that, unlike a dongle, several passwords or decryption keys can be written into the card so that the PC can use several software programs simultaneously. The Java card has the advantage that data can be written into it by an ordinary PC, through an ordinary card reader, unlike an ordinary smart card which requires special hardware to enable data to be written into it.

In order to make the sale to the purchaser, the retailer will take out a copy of the CD-ROM software and load it on the computer 1. He will also take the smart card or Java card 8 from the purchaser and insert it into the card reader/writer 2. The computer 1 of the retailer can write into a smart card or a Java card 8 using the card reader/writer 2. The retailer then logs onto the remote computer 4. When the computer 1 is connected to the remote computer 4 and the authenticity of the retailer has been validated using the retailers secure password, the retailer can access the registry on the remote computer 4. The remote computer 4 then sends a Java applet with a decryption key that will decrypt the software on the CD-ROM on the retailer's computer 1. Also contained in the Java applet is a password that will enable the decrypted software to run, similar to the password in a dongle, as described above. The decryption key and the password is written into the smart card or the Java card 8 by the computer 1 using the card reader/writer 2. Having done this, the retailer gives the CD-ROM and smart card or Java

card 8 to the purchaser.

In the manufacturer's registry on the remote computer 4, a record is made of the sale of the CD-ROM with its unique number against a unique identification of the purchaser. If another retailer or other person logs onto the remote computer 4 and asks to register the same CD-ROM, the remote computer 4 sends a message to warn the other retailer or person that the CD-ROM is pirated. Alternatively, there may be a genuine reason why the same CD-ROM needs to be re-registered. One reason could be that the purchaser has lost his smart card or Java card 8 or he wants to re-sell the software to another party. The manufacturer can have a policy with regard to multiple registrations of one CD-ROM. He can charge a price for it, as if he is re-selling the same software, or he can stipulate that the CD-ROM is destroyed and a new copy of the software on a new CD-ROM with a different registration be issued.

The remote computer 4 where the registry is kept is highly secured with encryption and decryption of data transmission between the remote computer 4 and the retailer's computer 1 and protected by a fire wall. As it may not be possible to have only one computer 4 to serve all the retailers across the world, multiple sites may be provided, for example, on the Internet. These may be hosted by different Internet service providers. Concurrency of data is maintained across the sites by means of data mirroring and replication

techniques. The sites can also serve as the platforms to transmit software to purchasers directly by means of electronic commerce.

After the purchaser purchases the CD-ROM, he loads the software on the CD-ROM into his computer 10 (see Figure 2) and inserts the smart card or Java card 8 into a card reader 11. The encrypted program on the CD-ROM is copied from the CD-ROM onto a hard disk 13 of the computer 10 and the decryption key is retrieved from the smart card or Java card 8 via a central processing unit (CPU) 12. The decrypted executable program is then permanently stored on the hard disk 13.

When the software is run on the computer 10, there is a routine to verify the password in the smart card or Java card 8 to make sure that only one copy is run and not multiple copies in several computers simultaneously. If the password check fails, the software will not run on the computer.

If the software is used with a Java card, as an added measure of security, the most essential part of the main executable program can be omitted from the CD-ROM. When the CD-ROM is sold, this critical part of the program can be downloaded from the remote computer 4, together with the decryption key and the password and stored on the Java card. When the software is run, the main executable program calls for this essential part to be retrieved from the Java card. This

enhances the security of the system as the software will not run without the portion of the software stored on the Java card, as the main executable program is not complete.

As an alternative to the software being sold and distributed in CD-ROM format, a user can have an authentication device 8 authenticated for specific software by an appropriate retailer. The purchaser may then use the authentication device 8 to download software from a remote computer 14 for example via the Internet 15, and install the software using the authentication device. If the authentication device 8 has not been correctly authenticated then the software will not install correctly on the user's computer 10.

Alternatively, or in addition, the authentication information for the software may be downloaded directly from the remote computer 14. In this example, the purchaser logs onto the remote computer 14 (for example via the Internet) and asks to purchase specific software. A Java applet from the remote computer 14 is sent to the purchaser's computer 10 to interrogate the Java card or smart card 8 for a unique identification and credit card number.

The credit card account identification may be embedded in the PC through software supplied to the purchaser by the credit card issuer. This would be secure software, which the purchaser could not tamper with.

The unique identification is authenticated against the credit card account identification in the purchaser's computer 10. After this is validated, a request is made to a credit card computer to make a deduction equivalent to the price of the software. If this is successful, a message is sent to the purchaser to confirm the transaction and be prepared to receive the software to be downloaded. The software is encrypted, and downloaded to the purchaser's computer 10. This is followed by the decryption key and the password which are written to the purchaser's Java card by the computer 10.

Currently, only Java cards can be written to by an ordinary computer. Hence, the above process can only work with a Java card. If the purchaser has a smart card, the process must stop after the encrypted software is downloaded. The buyer then has to go to the nearest retailer that is licensed to sell that software with the smart card. The retailer inserts the smart card into the card reader/writer 2 connected to the computer 1 and downloads a decryption key and password from the remote computer 4, as described above. In the registry will be the purchaser's identification and the unique number of the copy of the software downloaded. The decryption key and the password is then sent to the retailer's computer 1 in the form of a Java applet and written into the smart card.

A further example of the system is for supplying software for use on a network server. In this example, the retailer sells

the network version of the software to the purchaser. The software is supplied encrypted with a fixed number of smart cards or Java cards 8 that contain the decryption key and password for the software. The sale is registered with the registry of the software manufacturer before the key and password are downloaded from the remote computer 4, as before. The number of smart cards or Java cards 8 is at least equal to the number of concurrent users licensed to use the network software. The buyer loads the software onto the network server and distributes the smart cards or Java cards to users of the software on the server.

When a computer on the network requests the server for a copy of the software, the encrypted copy is sent to the computer. With the decryption key and the password in the smart card or Java card 8, the user is able to use the software.

Advantages of the invention are that it permits authentication information for a number of different software programs to be held on a single authentication device, and the software can not be used without the correct decryption key and the appropriate password. Hence, if a person only has a copy of the software and either no decryption key or the wrong password, the software will not operate. Hence, the invention reduces the likelihood of software being illegally copied, for example by making copies of a CD-ROM, as the CD-ROM is useless without the appropriate password and decryption key.

A further advantage is that the user can use the software on any computer provided that the identification device is used in conjunction with the software. This enables a user to run the software on any computer but also has the advantage of ensuring that the software can only run on on computer at any one time as the identification device is required to run the software.

CLAIMS

1. A computer software activation system comprising an authentication device, a writing device for writing to the authentication device, the writing device being coupled to a first computer, the first computer controlling the writing device to write authentication information to the authentication device, the authentication information written to the authentication device permitting corresponding software to be activated on a second computer.

2. A computer software activation system according to Claim 1, wherein the first computer accesses a remote computer to obtain the authentication information from the remote computer, and the authentication information obtained is written by the first computer to the authentication device via the writing device.

3. A computer software activation system according to Claim 2, wherein the connection between the first computer and the remote computer is a secure connection.

4. A computer software activation system according to Claim 2 or 3, wherein the information passed between the remote computer and first computer is encrypted.

5. A computer software activation system according to any of the preceding claims, wherein the authentication device

stores authentication information relating to a number of different computer software programs.

6. A computer software activation system according to any of the preceding claims, wherein the authentication device contains a processor.

7. A computer software activation system according to Claim 6, wherein the authentication device is a Smart Card or a Java Card.

8. A method of authenticating computer software comprising inserting an authentication device into an authentication device reader coupled to a computer on which the software is installed, the computer, in response to a request from the software for authentication information, obtaining from the authentication device reader the authentication information from the authentication device prior to or during initialisation of the software, the computer supplying the authentication information to the software and the software confirming to the computer that the authentication information from the authentication device permits the software to be run on the computer.

9. A method according to Claim 8, wherein the authentication device stores authentication information relating to a number of different computer software programs.

10. A computer software activation system according to any of claims 1 to 7, or a method of authenticating computer software according to claim 8 or claim 9, wherein the authentication information comprises a password.

11. A computer software activation system according to any of claims 1 to 7, or a method of authenticating computer software according to any of claims 8 to 10, wherein the software is encrypted and the authentication information comprises a decryption key to permit decryption of the software.

12. A computer software activation system according to any of claims 1 to 7, or a method of authenticating computer software according to any of claims 8 to 11, wherein the authentication information comprises a portion of the software without which the software will not operate.

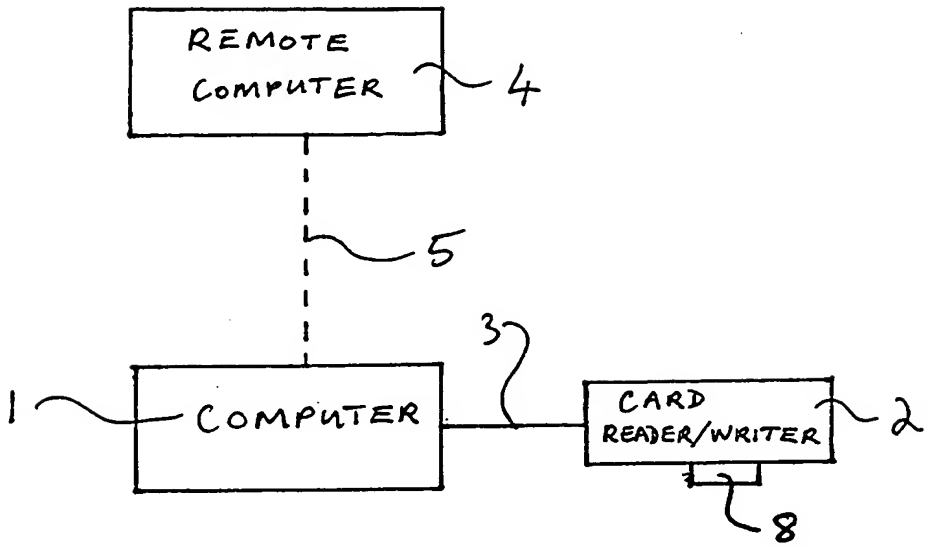


Figure 1

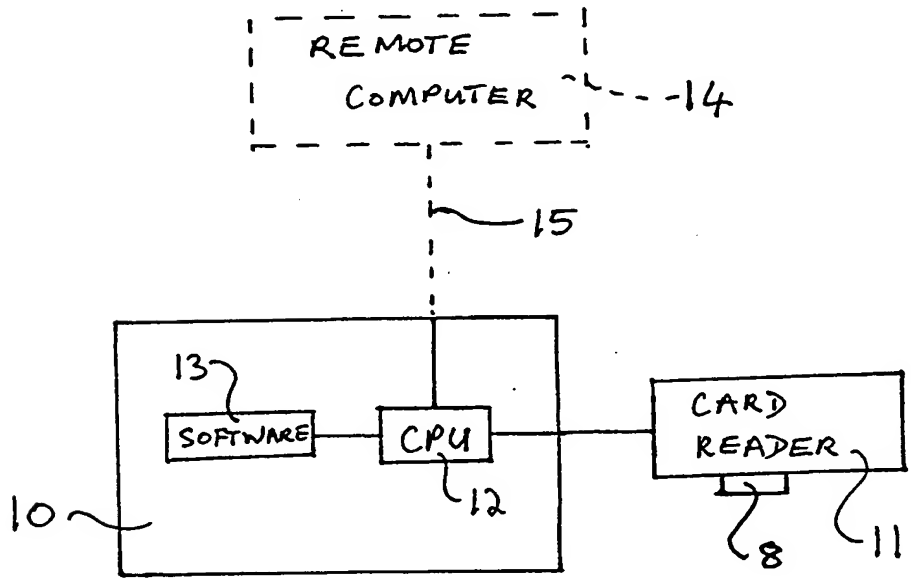


Figure 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00047

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6]: G 06 F 12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[6]: G 06 F 12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 191 162 A (IBM) 20 August 1986 (20.08.86), abstract.	1-11
A	US 5 666 411 A (MCCARTY) 09 September 1997 (09.09.97), abstract.	1
A	EP 0 808 048 A (AT & T) 19 November 1997 (19.11.97), abstract.	1
A	US 5 319 705 A (HALTER) 07 June 1994 (07.06.94), abstract.	1
A	US 5 588 146 A (LEROUX) 24 December 1996 (24.12.96), abstract.	1
A	US 5 416 840 A (HIRSCHMANN) 16 May 1995 (16.05.99), abstract.	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 1999 (10.05.99)	21 May 1999 (21.05.99)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer Fastenbauer Telephone No. 1/53424/447

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG 98/00047

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
EP 191162		CA A1 1238427	21-06-1988
		DE C0 3587072	18-03-1993
		DE T2 3587072	12-08-1993
		EP A2 191162	20-08-1986
		EP A3 191162	08-03-1989
		EP B1 191162	03-02-1993
		JP A2 61145642	03-07-1986
		JP B4 2060007	14-12-1990
		US A 4757534	12-07-1988
US A 5666411	09-09-1997	keine - none - rien	
EP 808048		CA AA 2201999	15-11-1997
		EP A2 808048	19-11-1997
		JP A2 10107895	24-04-1998
US A 5319705	07-06-1994	JP A2 7093148	07-04-1995
US A 5588146	24-12-1996	EP A1 594493	27-04-1994
		FR A1 2697357	29-04-1994
		FR B1 2697357	23-12-1994
		JP A2 6332717	02-12-1994
		SG A1 48122	17-04-1998
US A 5416840	16-05-1995	keine - none - rien	